View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

© Gnatyuk V., Terentyeva I., Kotelyanets V. Model of data for improving cybersecurity IP-PBX // Ukrainian Scientific Journal of Information Security, 2018, vol. 24, issue 3, pp. 175-180.

# КІБЕРБЕЗПЕКА ТА ЗАХИСТ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ / CYBERSECURITY & CRITICAL INFORMATION INFRASTRUCTURE PROTECTION

**DOI:** 10.18372/2225-5036.24.13428

# МОДЕЛЬ ДАНИХ ДЛЯ УДОСКОНАЛЕННЯ КІБЕРБЕЗПЕКИ IP-АТС

**Віктор Гнатюк[1], Ірина Терентьєва[1], Віталій Котелянець[2]**

*[1]Національний авіаційний університет, Україна*
*[2]Центральноукраїнський національний технічний університет, Україна*

**ГНАТЮК Віктор Олександрович,** к.т.н.

*Рік та місце народження:* 1990 рік, м. Нетішин, Хмельницька область, Україна.
*Освіта*: Хмельницький національний університет, 2012 рік.
*Посада:* доцент кафедри телекомунікаційних систем з 2017 року.
*Наукові інтереси:* інформаційна безпека, управління кіберінцидентами, телекомунікаційні системи та мережі.
*Публікації:* більше 50 наукових публікацій, серед яких наукові статті, тези та матеріали доповідей на конференціях, авторські свідоцтва.
*E-mail:* viktorgnatyuk@ukr.net

**ТЕРЕНТЬЄВА Ірина Євгенівна,** к.т.н.

*Рік та місце народження:* 1976 рік, м. Київ, Україна.
*Освіта:* Київський міжнародний університет цивільної авіації, 1999 рік.
*Посада:* доцент кафедри телекомунікаційних систем з 2018 року.
*Наукові інтереси:* математичне моделювання експлуатаційної надійності, оцінка ефективності експлуатації радіотехнічних і телекомунікаційних систем.
*Публікації:* 24 наукові публікації, серед яких наукові статті, тези та матеріали доповідей на конференціях, в тому числі три публікації, які увійшли у наукометричну базу Scopus.
*E-mail:* i.terentyeva@ukr.net

**КОТЕЛЯНЕЦЬ Віталій Володимирович**

*Рік та місце народження:* 1980 рік, м. Київ, Україна.
*Освіта*: Національний авіаційний університет, 2012 рік.
*Посада:* здобувач ЦНТУ.
*Наукові інтереси:* інформаційні технології, телекомунікаційні системи та мережі.
*Публікації:* більше 20 наукових публікацій, серед яких наукові статті, тези та матеріали доповідей на конференціях.
*E-mail:* kvvbud7@gmail.com

***Анотація.*** *Сучасний стан розвитку інформаційно-телекомунікаційних систем вражає своїми темпами впровадження, сферами застосування та різноманітністю технологій. Впровадження IP-телефонії у різні сфери людської діяльності дозволяє, для пересічних громадян, спростити побут, для бізнесу реалізувати головні аспекти такі як: збільшення продаж, підвищення ефективності роботи співробітників, підвищення якості обслуговування клієнтів, автоматизація робочих процесів, представлення необхідної інформації для керівництва тощо. Дана технологія (IP-телефонія) стала яскравим симбіозом класичної телефонії та мережі Інтернет, поєднала в собі всі найважливіші функції зазначених технологій. Проте, використовуючи IP-телефонію важливо подбати про забезпечення необхідного рівня кібербезпеки, оскільки не виконання цього ас-*

*пекту може нести з собою великі фінансові та іміджеві втрати, тому розробка і дослідження нових ефективних методів удосконалення кібербезпеки IP-телефонії є актуальною задачею. Тому, метою даної роботи є побудова моделі даних для удосконалення кібербезпеки IP-АТС. Для досягнення мети, сформуємо множину видів вразливостей IP-АТС, множину кроків для реалізації кібератаки на IP-АТС та множину дій для удосконалення кібербезпеки IP-АТС, що дозволить ідентифікувати можливі види вразливостей для IP-АТС, дослідити послідовність кроків для реалізації кібератаки на IP-АТС та виконавши превентивні дії удосконалити рівень кібербезпеки IP-АТС. Для успішної реалізації кібератаки, за налаштувань, що представлені в статті, потрібна дуже висока кваліфікація зловмисників та значні матеріально-технічні затрати. Розроблена модель буде корисною, насамперед, для системних адміністраторів, а також для фахівців з інформаційної безпеки у складі команд реагування на кіберінциденти типу CERT/CSIRT на які покладаються обов'язки щодо захисту ІТС в межах підприємств та організацій.*

***Ключові слова:*** *IP-телефонія, кіберінцидент, Asterisk, SIP, АТС.*

**Вступ**

Сьогодні людство отримало в своє розпорядження досить багато цікавих сучасних технологій, зокрема IP-телефонія, яка для пересічних громадян дозволяє спростити побут, для бізнесу реалізувати головні аспекти: збільшити продажі, підвищити ефективність роботи співробітників, підвищити якість обслуговування клієнтів, автоматизувати робочі процеси, надати необхідну інформацію для керівництва тощо. Дана технологія стала яскравим симбіозом класичної телефонії та мережі Інтернет. Вона поєднала в собі всі найважливіші функції зазначених технологій. Проте, використовуючи IP-телефонію важливо подбати про забезпечення необхідного рівня кібербезпеки, оскільки не виконання цього аспекту може нести з собою великі фінансові та іміджеві втрати, тому розробка і дослідження нових ефективних методів удосконалення кібербезпеки IP-телефонії є *актуальною* науковою задачею.

Принцип функціонування IP-телефонії полягає в тому, що голос абонента автоматично трансформується в пакети даних, які передаються через мережу до заданого адресату і відразу після цього перетворюються знову на звичайну мову. Телефонія даного типу прямо відноситься до більш широкої категорії, що отримала назву VoIP (Voice Over IP). Остання дозволяє передавати за таким же принципом не лише стандартні голосові повідомлення, а і дає можливість відправляти всілякі відеофайли і подібні послання. Така технологія дозволяє в кілька разів мінімізувати навантаження на мережу. Паралельно з цим зменшується і вартість стаціонарного телефонного дзвінка. Для того, щоб скористатися перевагами IP-телефонії, потрібно обзавестися спеціально розробленими пристроями. Такими є SIP-телефони і софтфони. Виробництвом обладнання даного напрямку займається не так багато підприємств. Особливо великих успіхів змогли досягти Grandstream і Cisco SB. Торгові марки випускають широкий асортимент пристроїв для IP-телефонії, постійно покращуючи якість товарів. В каталог включені моделі IP-телефонів з такими конструктивними особливостями: з провідною трубкою, бездротові, з ЖК-дисплеєм, з Wi-Fi тощо. Кожна така функціональна особливість забезпечує зручність користування пристроєм даного призначення.

**Аналіз рішень та постановка задачі**

Сьогодні на ринку представлено велику кількість рішень для побудови IP-телефонії (Asterisk, 3CX, Oktell тощо), проте беззаперечним лідером є вільне рішення комп'ютерної телефонії (в тому числі, VoIP) з відкритим вихідним кодом Asterisk від компанії Digium. Архітектура системи Asterisk (рис. 1) включає: мережу, обладнання, локальну операційну систему та компоненти [1].

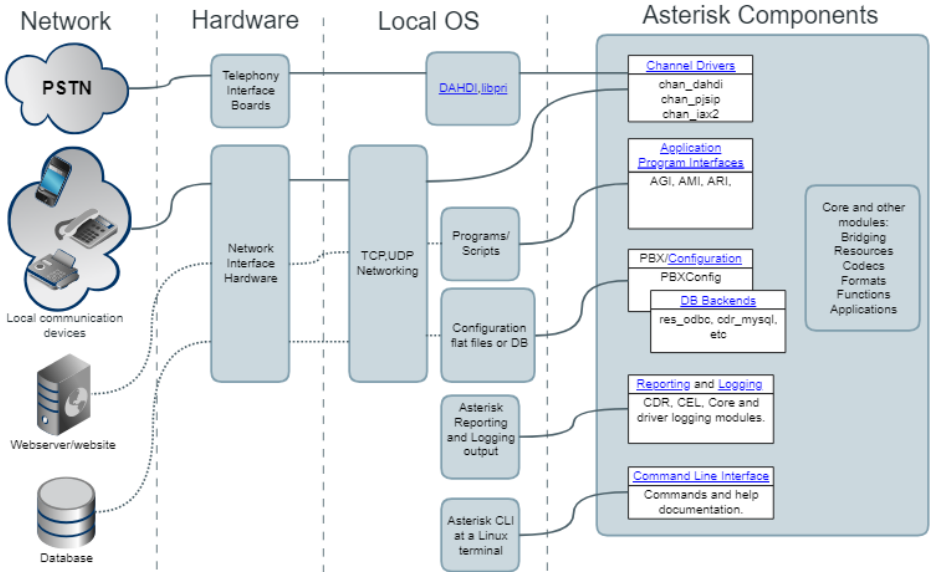


Рис. 1. Архітектура системи Asterisk

Asterisk в комплексі з необхідним обладнанням має всі можливості класичної АТС, підтримує безліч VoIP протоколів (SIP, H.323, IAX2, MGCP, SIMPLE, SCCP, XMPP, Unistim) і надає функції управління дзвінками (голосова пошта, конференц зв'язок, IVR, центр обробки дзвінків, Call Detail Record), можливо також транслювати текст і відеосигнали. Підтримка широкого спектру обладнання та комп'ютерних протоколів дозволяє організовувати величезну кількість сценаріїв взаємодії мереж, отримання і обробки інформації. Asterisk може працювати як з аналоговими лініями (FXO / FXS модулі), так і цифровими (ISDN, BRI і PRI - потоки T1/E1). За допомогою певних комп'ютерних плат Asterisk можна підключити до високопропускних ліній T1/E1, які дозволяють працювати паралельно з десятками телефонних з'єднань. Повний список обладнання для з'єднання з телефонною мережею загального користування визначається підтримкою обладнання в модулях ядра. Типова схема організації IP телефонії Asterisk зображена на рисунку 2.

Використовуючи IP-АТС Asterisk важливо подбати про забезпечення необхідного рівня кібербезпеки, оскільки не виконання цього аспекту може нести з собою великі фінансові та іміджеві втрати. Як правило, «зламують», реалізують кіберінциденти [2], Asterisk з інших країн і починають здійснювати міжнародні дзвінки, після таких «зломів», організаціям приходять рахунки на десятки і навіть сотні тисяч у.о. Причому жертвою може стати як і велика організація (що не факт), так і маленька. В основному це дрібні організації, де безпеці Asterisk приділяється мінімальна увага. Сканування мережі Інтернет у пошуках чергової жертви триває постійно. Отримавши доступ до Asterisk, зловмисники можуть під'єднувати цілі організації на аккаунт жертви і здійснювати міжнародні дзвінки за їх рахунок. Тому, метою даної роботи є побудова моделі даних для удосконалення кібербезпеки IP-АТС. Для досягнення мети, сформуємо множину видів вразливостей IP-АТС, множину кроків для реалізації кібератаки на IP-АТС та множину дій для удосконалення кібербезпеки IP-АТС, що дозволить ідентифікувати можливі види вразливостей для IP-АТС, дослідити послідовність кроків для реалізації кібератаки на IP-АТС та виконавши превентивні дії удосконалити рівень кібербезпеки IP-АТС.

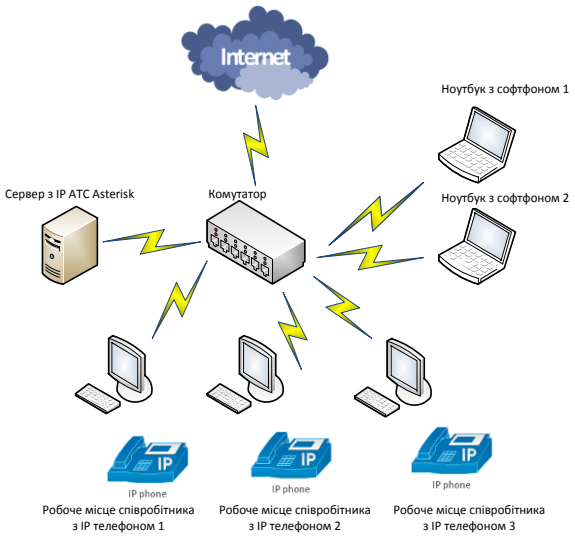


Рис. 2. Схема організації IP телефонії Asterisk

**Формування множини видів вразливостей.** Задамо множину видів вразливостей $\mathbf{V}$, які існують під час функціонування IP-АТС:

$$\mathbf{V} = \{\bigcup_{i=1}^{n} \mathbf{V}_i\} = \{\mathbf{V}_1, \mathbf{V}_2, ..., \mathbf{V}_n\}, \quad (i = \overline{1,n}), \tag{1}$$

де $n$ – кількість можливих видів вразливостей.

Наприклад, в результаті проведення аналізу існуючих видів вразливостей під час функціонування IP-АТС [3-11] сформуємо таблицю для IP-АТС Asterisk табл. 1.

Отже, використовуючи вираз (1) та дані з табл. 1, при $n = 11$ отримаємо:

$$\begin{aligned} \mathbf{V}_A &= \{\bigcup_{i=1}^{n} \mathbf{V}_i\} = \{\mathbf{V}_1, \mathbf{V}_2, \mathbf{V}_3, \mathbf{V}_4, \mathbf{V}_5, \mathbf{V}_6, \mathbf{V}_7, \mathbf{V}_8, \mathbf{V}_9, \mathbf{V}_{10}, \mathbf{V}_{11}\} = \\ &= \{\mathbf{V}_{NCF}, \mathbf{V}_{DP}, \mathbf{V}_{SP}, \mathbf{V}_{BSF}, \mathbf{V}_{FSD}, \mathbf{V}_{FSA}, \mathbf{V}_{SA}, \mathbf{V}_{LE}, \mathbf{V}_{AV}, \mathbf{V}_{ICA}, \mathbf{V}_{LF}\} = \\ &= \{NCF, DP, SP, BSF, FSD, FSA, SA, LE, AV, ICA, LF\}, \end{aligned} \tag{2}$$

де $\mathbf{V}_1 = \mathbf{V}_{NCF} = NCF$, $\mathbf{V}_2 = \mathbf{V}_{DP} = DP$, …, $\mathbf{V}_{11} = \mathbf{V}_{LF} = LF$ – види вразливостей для IP-АТС Asterisk.

Таблиця 1

Види вразливостей для IP-АТС Asterisk

| № | Код | Опис |
|---|---|---|
| 1 | NCF | Asterisk з певних причин має виділену IP адресу і відображається в мережі Інтернет (наприклад, цей сервер Asterisk так само є і сервером, що роздає Інтернет, так, що провід з Інтернетом і виділеним «білим» IP вставлений прямо в цей сервер). При цьому, на сервері з Asterisk не налаштований фаервол, і цей Asterisk вразливий зі сторони мережі. |
| 2 | DP | На SSH і SIP призначені порти за замовчуванням. |
| 3 | SP | Використовуються прості паролі для SIP клієнтів. |
| 4 | BSF | Не включена функція захисту від перебору існуючих SIP клієнтів. |
| 5 | FSD | Не реалізована функція захисту на рівні Dial плану. |
| 6 | FSA | Не реалізована функція доступу тільки з локальної мережі. |
| 7 | SA | За SSH дозволений доступ root користувача. |
| 8 | LE | У Linux не відключені непотрібні служби з дірками. |
| 9 | AV | Використовується система з PBX-інтерфейсом, наприклад Elastix, яка має додаткові уразливості. |
| 10 | ICA | На рівні SIP провайдера дозволені міжнародні дзвінки (коли вони не потрібні). |
| 11 | LF | На рівні SIP провайдера не реалізована функція обмеження (дзвони скільки хочеш, але в кінці місяця отримаєш рахунок). |

**Формування множини кроків для реалізації кібератаки.** Для реалізції цього етапу задамо множину кроків $\mathbf{S}$ :

$$\{\bigcup_{j=1}^{m}\mathbf{S}_j\}=\{\mathbf{S}_1,\mathbf{S}_2,...,\mathbf{S}_m\}, \quad 3)$$

де $\mathbf{S}_j \subseteq \mathbf{S}$ , $(j=\overline{1,m})$ , $m$ – кількість кроків зловмисника.

Наприклад, розглянемо послідовність кроків для реалізації кібератаки на IP-ATC Asterisk (табл. 2).

Отже, використовуючи вираз (3) та дані з табл. 2, при $n=5$ отримаємо:

$$\mathbf{S}_A=\{\bigcup_{i=1}^{5}\mathbf{S}_i\}=\{\mathbf{S}_1,\mathbf{S}_2,\mathbf{S}_3,\mathbf{S}_4,\mathbf{S}_5\}= \quad (4)$$
$$=\{\mathbf{S}_{SC},\mathbf{S}_{SL},\mathbf{S}_{BF},\mathbf{S}_{SR},\mathbf{S}_{MC}\}=\{SC,SL,BF,SR,MC\},$$

де $\mathbf{S}_1=\mathbf{S}_{SC}=SC$ , $\mathbf{S}_2=\mathbf{S}_{SL}=SL$ , $\mathbf{S}_3=\mathbf{S}_{BF}=BF$ , $\mathbf{S}_4=\mathbf{S}_{SR}=SR$ , $\mathbf{S}_5=\mathbf{S}_{MC}=MC$ – кроки зловмисника для реалізації кібератаки на IP ATC Asterisk.

**Формування множини дій для удосконалення кібербезпеки IP-ATC.**

Для реалізції цього етапу задамо множину дій $\mathbf{A}$ для удосконалення кібербезпеки IP-ATC:

$$\mathbf{A}=\{\bigcup_{d=1}^{v}\mathbf{A}_d\}=\{\mathbf{A}_1,\mathbf{A}_2,...,\mathbf{A}_v\}, \quad (5)$$

де $\mathbf{A}_d \subseteq \mathbf{A}$ , $(d=\overline{1,v})$ , $v$ – кількість дій для удосконалення кібербезпеки IP-ATC.

Наприклад, розглянемо дії для удосконалення кібербезпеки IP-ATC Asterisk табл. 3.

Таблиця 2

Опис кроків для реалізації кібератаки на IP-ATC Asterisk

| № | Код | Опис |
|---|---|---|
| 1 | **SC** | Сканування мережі Інтернет на наявність систем з відкритим портом 5060 (клієнти SIP традиційно використовують порт 5060 TCP і UDP для з'єднання серверів та інших елементів SIP. В основному SIP використовується для встановлення і роз'єднання голосових і відеодзвінків). |
| 2 | **SL** | Система (Asterisk) знайдена, пошук наявних SIP клієнтів, до яких можна підключитися. Відправлення запитів, поки не прийде відповідь про те, що такий SIP клієнт існує. У підсумку, зловмисник отримує список виду: [1000] [1001] [1002] - це SIP клієнти. |
| 3 | **BF** | Запуск «брутофорс» – програми підбору пароля до SIP клієнтів. |
| 4 | **SR** | Знайшовши пароль, зловмисник запускає у себе на комп'ютері софтфон і реєструє його за отриманими даними - зовнішньою IP адресою (яку він знайшов скануючи відкриті 5060 порти, логін (який такий же, як і номер знайденого ним SIP-клієнта) і пароль, який він підібрав в результаті «брутофорса». |
| 5 | **MC** | Зловмисник може здійснювати міжнародні дзвінки, тощо. |

Таблиця 3

Дії для удосконалення кібербезпеки IP-ATC Asterisk

| № | Код | Опис |
|---|---|---|
| 1 | CS | Зміна SIP порта (bindport = 3348;) |
| 2 | SL | Заборона SIP підключень за межами локальної мережі<br>(deny = 0.0.0.0 / 0.0.0.0;<br>permit = 192.168.0.1 / 24;<br>allowguest = no;<br>call-limit = 2;) |
| 3 | SS | Захист серверу від перебору за номерами (Alwaysauthreject = yes) |
| 4 | IC | Встановлення складних паролів для SIP-клієнтів (можна використати генератор паролів, пароль зі службовими знаками і цифрами) |
| 5 | SI | Заборона міжнародних викликів на рівні Dial плану<br>(exten => _3809X.,1,System(echo «To» ${EXTEN} «Ext» ${CALLERID(num)} \| mail -s «8-10 ALARM» test@gmail.com);<br>exten => _3809X.,n,Hangup();) |
| 6 | CF | Налаштування вбудованого фаєрволла iptables (редагування конфігураційного файлу iptables) |
| 7 | CP | Зміна порту SSH, заборона користувачеві «логінитися» як root через SSH, додаємо нового користувача (useradd username, passwd username; AllowUsers username, PermitRootLogin no; Port 1265) |
| 8 | DA | Вимикаємо Apache з автозавантаження і змінюємо його порт (chkconfig httpd off, IP_адрес_сервера: 7623) |
| 9 | DM | Відключаємо непотрібні модулі і протоколи Asterisk<br>(noload => chan_jingle.so<br>noload => chan_skinny.so<br>noload => chan_iax2.so<br>noload => chan_console.so<br>noload => chan_mgcp.so<br>noload => chan_gtalk.so) |
| 10 | CM | Змінимо порт управління Asterisk (AMI) (port = 8374) |
| 11 | SF | Налаштовуємо систему fail2ban (програма захисту серверів від атаки «Brute force»). |

Продовження таблиці 3

| № | Код | Опис |
|---|---|---|
| 12 | SD | Захист від DOS атак (модифікуємо iptables):<br>(-A INPUT -p tcp -m multiport --dports 1265,7623,3348,137,138,139,445 -m recent --set --name dos-attack<br>-A INPUT -p tcp -m multiport --dports 1265, 7623,3348,137,138,139,445 -m recent --update --seconds 2 --hitcount 20 --name dos-attack -j DROP)<br>Також, можна пов'язати роботу iptables з системою fail2ban таким чином, щоб пакети від DOS атаки не відкидалися, а повідомлення про них записувалися в лог файл iptables. Fail2ban на підставі шаблону, переглядає лог / var / log / messages і якщо він бачить таке повідомлення в цьому лозі, просто блокує IP адресу яка посилає ці повідомлення і повідомляє нас на e-mail про те, що була здійснена DOS атака. |
| 13 | SSP | Захист від сканування портів (iptables - xtables-addons) |
| 14 | SSH | Сертифікація SSH. Існує можливість зробити так, щоб підключитися по SSH (наприклад, через Putty) можна було б тільки якщо на комп'ютері, з якого підключаються до сервера Linux встановлений сертифікат. Загальна процедура наступна: 1) Генерується ключі. 2) Згенерований ключ заноситься в файл authorized_keys. 3) Згенерований ключ витягується з Linux в Windows. 4) Витягнений згенерований ключ за допомогою програми puttygen перетворюється. 5) Отриманий перетворений файл підключається до Putty. 6) Настроюється сама служба SSH в Linux. 7) Перевірка працездатності. |
| 15 | ES | Відключення samba (; Path; chkconfig smb off) |
| 16 | DP | На рівні провайдера також можлива: заборона міжнародних дзвінків, встановлення лімітів, обмеження максимальної вартості дзвінків. |
| 17 | OE | Встановлення захищеного VPN з'єднання, встановлення складних паролів до веб-інтерфейсів апаратних телефонів, зміна HTTP порту. |

Отже, використовуючи вираз (5) та дані з табл. 3, при $n = 17$ отримаємо:

$$\mathbf{A}_A = \{\bigcup_{i=1}^{17} \mathbf{A}_i\} = \{\mathbf{A}_1, \mathbf{A}_2, \mathbf{A}_3, \mathbf{A}_4, \mathbf{A}_5, \mathbf{A}_6, \mathbf{A}_7, \mathbf{A}_8, \mathbf{A}_9, \mathbf{A}_{10}, \mathbf{A}_{11}, \mathbf{A}_{12}, \mathbf{A}_{13}, \mathbf{A}_{14}, \mathbf{A}_{15}, \mathbf{A}_{16}, \mathbf{A}_{17}\} =$$
$$= \{\mathbf{A}_{CS}, \mathbf{A}_{SL}, \mathbf{A}_{SS}, \mathbf{A}_{IC}, \mathbf{A}_{SI}, \mathbf{A}_{CF}, \mathbf{A}_{CP}, \mathbf{A}_{DA}, \mathbf{A}_{DM}, \mathbf{A}_{CM}, \mathbf{A}_{SF}, \mathbf{A}_{SD}, \mathbf{A}_{SSP}, \mathbf{A}_{SSH}, \mathbf{A}_{ES}, \mathbf{A}_{DP}, \mathbf{A}_{OE}\} = \quad (6)$$
$$= \{CS, SL, SS, IC, SI, CF, CP, DA, DM, CM, SF, SD, SSP, SSH, ES, DP, OE\},$$

де $\mathbf{A}_1 = \mathbf{A}_{CS} = CS$ , $\mathbf{A}_2 = \mathbf{A}_{SL} = SL$ , …, $\mathbf{A}_{17} = \mathbf{A}_{OE} = OE$ – дії для удосконалення кібербезпеки IP-АТС Asterisk.

Таким чином, виконавши дії зазначені у табл. 3 можна удосконалити кібербезпеку для IP-АТС Asterisk. Для успішної реалізації кібератаки, за таких налаштувань, потрібна дуже висока кваліфікація зловмисників та значні матеріально-технічні затрати.

**Висновки**

Таким чином, у цій роботі побудовано модель даних для удосконалення кібербезпеки IP-АТС, сформовано множину видів вразливостей IP-АТС, множину кроків для реалізації кібератаки на IP-АТС та множину дій для удосконалення кібербезпеки IP-АТС, що дозволяє ідентифікувати можливі види вразливостей для IP-АТС, дослідити послідовність кроків для реалізації кібератаки на IP-АТС та виконавши превентивні дії удосконалити рівень кібербезпеки IP-АТС.

Розроблена модель спрямована на те, щоб унеможливити реалізацію зловмисниками кіберінцидентів в IP-АТС. Ця модель буде корисною, насамперед, для системних адміністраторів, а також для фахівців з інформаційної безпеки у складі команд реагування на кіберінциденти типу CERT/CSIRT на які покладаються обов'язки щодо захисту ІТС в межах підприємств та організацій. В подальших дослідженнях планується встановлення зв'язків між видами вразливостей та діями для удосконалення кібербезпеки IP-АТС.

**Література**

[1]. Asterisk Architecture. [Електронний ресурс]. Режим доступу: https://wiki.asterisk.org/wiki/display/AST/Asterisk+Architecture%2C+The+Big+Picture.

[2]. В. Гнатюк, "Аналіз дефініцій поняття «інцидент» та його інтерпретація у кіберпросторі", *Безпека інформації,* №3 (19), С. 175-180, 2013.

[3]. Дж. Меггелен, Л. Мадсен, Дж. Сміт, *Asterisk™: майбутнє телефонії, 2-е видання. — Пер. з англ,* СПб: Символ-Плюс, 2009, 656 с.

[4]. М. Платов, "Asterisk і Linux - місія IP-телефонія", *Системний Адміністратор*, № 31, С. 10-38, 2005.

[5]. База знань Asterisk. [Електронний ресурс]. Режим доступу: asterisk.ru/knowledgebase.

[6]. База знань Voxlink. [Електронний ресурс]. Режим доступу: www.voxlink.ru/kb.

[7]. Безпека в VoIP мережах. [Електронний ресурс]. Режим доступу: habrahabr.ru/post/145206.

[8]. А. Росляков, М. Самсонов, І. Шибаєва, *IP-телефонія,* М.: Еко-Трендз, 2003, 252 с.

[9]. Б. Гольдштейн, А. Пінчук, А. Суховицького, *IP-телефонія,* М.: Радио и связь, 2001, 336 с.

[10]. CITForum. Безпека IP-телефонії - польові замальовки. [Електронний ресурс]. Режим доступу: citforum.ru/security/articles/ipsec.

[11]. 9 правил, як захистити свій Asterisk! [Електронний ресурс]. Режим доступа: https://habr.com/company/myasterisk/blog/130325/.

**УДК 004.7 (045)**

***Гнатюк В.А., Терентьева И.Е., Котелянец В.В. Модель данных для усовершенствования кибербезопасности IP-АТС***

***Аннотация.*** *Современное состояние развития информационно-телекоммуникационных систем (ИТС) поражает своими темпами внедрения, сферами применения и разнообразием технологий. Внедрение IP-телефонии в различных сферах человеческой деятельности позволяет, для рядовых граждан, упростить быт, для бизнеса реализовать главные аспекты такие как: увеличение продаж, повышение эффективности работы сотрудников, повышения качества обслуживания клиентов, автоматизация рабочих процессов, представление необходимой информации для руководства и др. Данная технология (IP-телефония) стала ярким симбиозом классической телефонии и сети Интернет, сочетающего в себе все важнейшие функции указанных технологий. Однако, используя IP-телефонию важно позаботиться об обеспечении необходимого уровня кибербезопасности, поскольку невыполнение этого аспекта может нести с собой большие финансовые и имиджевые потери, поэтому разработка и исследование новых эффективных методов совершенствования кибербезопасности IP-телефонии является актуальной задачей. Поэтому, целью данной работы является построение модели данных для усовершенствования кибербезопасности IP-АТС. Для достижения цели, сформируем множество видов уязвимостей IP-АТС, множество шагов для реализации кибератаки на IP-АТС и множество действий для совершенствования кибербезопасности IP-АТС, что позволит идентифицировать возможные виды уязвимостей для IP-АТС, исследовать последовательность шагов для реализации кибератаки на ИР АТС и выполнив превентивные действия усовершенствовать уровень кибербезопасности IP-АТС. Для успешной реализации кибератаки, после настроек, что представленные в статье, нужна очень высокая квалификация злоумышленников и значительные материально-технические затраты. Разработанная модель будет полезной, прежде всего, для системных администраторов, а также для специалистов по информационной безопасности в составе команд реагирования на киберинциденты типа Computer Emergency Response Team / Computer Security Incident Response Team на которые возлагаются обязанности по защите ИТС в пределах предприятий и организаций.*

***Ключевые слова:*** *IP-телефония, киберинцидент, Asterisk, SIP, АТС.*

***Gnatyuk V., Terentyeva I., Kotelyanets V. Model of data for improving cybersecurity IP-PBX***

***Abstract.*** *The current state of development of information and telecommunication systems is impressive with its pace of implementation, scope and variety of technologies. Introduction of IP-telephony in various spheres of human activity allows ordinary people to simplify their lives, implement the main aspects for business, such as: increasing sales, improving employee efficiency, improving customer service quality, automating work processes, presenting the necessary information for management, etc. This technology (IP-telephony) has become a vivid symbiosis of classical telephony and the Internet, combining all the most important functions of these technologies. However, using IP telephony is important to ensure the necessary level of cybersecurity, since failure to implement this aspect can lead to significant financial and image losses, so the development and research of new effective methods for improving the cyber security of IP-telephony is an urgent task. Therefore, the purpose of this work is to build a data model for improving the cyber security IP-PBX. To achieve the goal, we will create a variety of types of IP-PBX vulnerabilities, a set of steps to implement cyberattack on the IP-PBX and a set of actions to improve the cyber security of the IP-PBX, which will identify possible types of vulnerabilities for the IP-PBX, investigate the sequence of steps to implement cyberattacks on IP-PBX and after performing preventive actions to improve the level of cybersecurity IP-PBX. After setting up an IP telephony server, following the example presented in the article, successful implementation of a cyberattack requires a very high level of intruder qualification of hacker and significant logistical costs. The developed model will be useful, first of all, for system administrators, as well as for information security specialists in the response teams for cyber incidents such as Computer Emergency Response Team / Computer Security Incident Response Team, which are responsible for the security of information and telecommunication systems within enterprises and organizations.*

***Keywords:*** *IP-telephony, cyberincident, Asterisk, SIP, PBX.*

Отримано 29 *жовтня 2018 року*, затверджено редколегією 12 *грудня 2018 року*